UNIVERSIDAD AUTONOMA DE MADRID

ESCUELA POLITECNICA SUPERIOR

Grado en Tecnologías y Servicios de Telecomunicación

TRABAJO FIN DE GRADO

ADQUISICIÓN DE BASE DE DATOS Y DESARROLLO DE SISTEMA DE RECONOCIMIENTO BIOMÉTRICO BASADO EN FIRMA MANUSCRITA

Beatriz Cervantes Reyes
Tutor: Rubén Vera Rodríguez
Ponente: Javier García Ortega

JUNIO 2016

ADQUISICIÓN DE BASE DE DATOS Y DESARROLLO DE SISTEMA DE RECONOCIMIENTO BIOMÉTRICO BASADO EN FIRMA MANUSCRITA

AUTOR: Beatriz Cervantes Reyes
TUTOR: Rubén Vera Rodríguez

Biometric Recognition Group - ATVS
Dpto. de Tecnología Electrónica y de las Comunicaciones
Escuela Politécnica Superior
Universidad Autónoma de Madrid
Junio de 2016

Resumen

Este proyecto se basa en la adquisición y evaluación de una base de datos de firma dinámica con varios dispositivos fijos y móviles, y en dos sesiones separadas en el tiempo. Los dispositivos que se han utilizado para la captura de esta base de datos han sido un Smartphone y dos tabletas: una tableta WACOM, diseñada exclusivamente para la captura de firma dinámica mediante lápiz, y una tableta y smartphone con sistema operativo Android y de uso genérico.

Como punto de partida, se estudia el estado del arte. En esta parte se explican los distintos modos de operación en el reconocimiento biométrico. En el modo verificación, se hace especial hincapié en la arquitectura que presenta este tipo de sistema, comenzando por la etapa de captura de datos y terminando en la normalización de puntuaciones.

Una vez entendido el estado del arte desde el punto de vista teórico, el siguiente paso ha sido definir y describir el diseño de la base de datos. Esta base de datos es multisesión, multimodal, y lo suficientemente grande como para dar resultados fiables. Se han recogido firmas genuinas, muestras de escritura e imitaciones. Los usuarios que han realizado estas falsificaciones lo han hecho mediante distintos procedimientos, siendo unos más realistas que otros.

En el momento en el que la base de datos fue finalmente obtenida, se procedió a realizar la parte experimental. Este desarrollo experimental se ha llevado a cabo en dos etapas. Durante la primera etapa el objetivo fue evaluar el rendimiento del sistema de verificación de firma dinámica sin interoperabilidad. En este punto, se distinguen distintos tipos de comparaciones a la hora de evaluar el rendimiento del sistema, siendo la comparación de lápiz contra dedo una de las destacadas. En la segunda etapa, se estudió de nuevo el rendimiento del sistema pero en este caso, aplicando interoperabilidad entre los dispositivos, con el objetivo de conseguir un rendimiento lo más parecido posible al sistema sin interoperabilidad.

Finalmente, se presentan las conclusiones extraídas a lo largo de este trabajo, así como el posible trabajo futuro.

Palabras clave

Identificación, reconocimiento biométrico, e-Biofirma, autentificación, verificación, biometría, firma digital, tableta, smartphone, base de datos, interoperabilidad, Matlab, matching, entrenamiento, test, dispositivo, WACOM, Samsung, pen, dedo.

Abstract

This project is based on the acquisition and evaluation of a dynamic signature database with several types of devices, and in two sessions in time. The devices used to capture this database are a Smartphone and tablet with Android Operating System and general purpose, and Wacom tablet specifically designed to acquire dynamic signatures using a pen stylus.

To start up, we study the general architecture of a biometric recognition system, considering the different operational modes of identification and verification. In this project we consider a system working in a verification mode, and we pay attention to all the stages from the data capture to the scores normalization.

The next step was to define and describe the design of the database. This database is multisession, multi-modal, and large enough to provide reliable results. Samples of genuine signatures and handwriting names together with skilled forgeries. These skilled forgeries have been done by users utilizing several methods, being ones more realistic than others.

At the time the database was finally acquired, we proceeded to do the experimental part. This experimental development is carried out in two stages. During the first stage, the objective was to evaluate the performance of the verification system for dynamic signatures without interoperability. At this point, several types of comparisons can be distinguished when evaluating the system performance, being the comparison pencil against finger one of the leading ones. In the second stage, the system performance was studied again but in this case, applying interoperability between devices, with the aim of achieving the closest performance possible to the system in a no interoperability case.

Finally, the conclusions drawn throughout this work as well as possible future work are presented.

Keywords

Identification, biometric recognition, e-Biofirma, authentication, verification, biometrics, digital signature, tablet, smartphone, database, interoperability, Matlab, matching, training, testing, device, WACOM, Samsung, pen, finger

Gracias

En primer lugar, me gustaría agradecer a mi tutor Rubén Vera tanto la ayuda, como los consejos e ideas que me ha aportado a lo largo de este proyecto. También quiero dar las gracias a Javier Ortega, en primer lugar, por hacer que me entusiasme todo este mundo de la biometría y en segundo, por darme la oportunidad de realizar este proyecto. Agradecer también a todos aquellos que han participado en la adquisición de la base de datos, invirtiendo su tiempo y aguantándome en el proceso.

A lo largo de mi recorrido por la universidad, he conocido a muchos profesores de los cuales he aprendido muchas cosas como la transformada de Fourier, sistemas lineales, análisis de circuitos, etc. Pero sobre todo he aprendido a no rendirme, a luchar por lo que quiero, a esforzarme al máximo, a tener paciencia y a celebrar los éxitos. Porque no digo que haya sido fácil, pero sí puedo decir que ha merecido la pena.

No quiero nombrar a mis compañeros de la universidad, ya que hoy por hoy no los considero compañeros sino amigos, gracias a ellos este camino ha sido inolvidable, en algunas ocasiones les veía más que a mi familia, como no les voy a querer. Muchas gracias Calzada, Dani, Mario, Raúl García y Ricky. Y como olvidarme de mi mitad, Beatriz, que se ha convertido en una gran amiga, con ella he llorado, he reído, nos hemos desesperado y he vuelto a reír. Sin ti todo esto no hubiera sido lo mismo.

También dar las gracias a mis "angeles de chirly" por mantenerme la sonrisa en momentos de agobio y recordarme el verdadero valor de la amistad. Por siempre chicas.

A él, mi chico, por apoyarme, por ese "tú puedes con todo y más", por levantarme, por sacarme una sonrisa, por secarme las lágrimas, por ayudarme y sobre todo por estar siempre ahí. Muchas gracias Alex.

Pero sobre todo se lo quiero agradecer a ellos, mi gran familia. Gracias por confiar en mí aun cuando ni yo lo hacía, por darme todo lo mejor, por acompañarme en el camino de la vida y hacerlo mucho más bonito, por ser mi gran ejemplo a seguir. Teníais razón, todo esfuerzo merece su recompensa. Mi recompensa no es esto, sino teneros a todos vosotros. Os quiero.

A cada uno de vosotros, os dedico este trabajo. Gracias

Beatriz Cervantes Reyes
Junio 2016

Índice general

Índice de figuras

Índice de tablas

Preámbulo

Glosario de acrónimos

- **FAR:** False Acceptance Rate
- **FRR:** False Reject Rate
- **EER:** Equal Error Rate
- **DET:** Detection Error Tradeoff
- **HMM:** Hidden Markov Models
- **DTW:** Dinamic Time Warping
- **UAM:** Universidad Autónoma de Madrid

Herramientas utilizadas

- **Lenguajes de programación:** Matlab.
- **Programas utilizados:** Eclipse.

Notaciones utilizadas

Se han utilizado las siguientes abreviaturas: Sec. (Sección), Fig. (Figura) y Ecu (Ecuación).

1| Introducción

1.1 Motivación del proyecto

La problemática que motiva el uso de sistemas de reconocimiento de la identidad, los cuales tienen como entrada la firma como rasgo biométrico usando su información dinámica, es:

- **Necesidad de aumentar la seguridad.** Es sabido por todos, que la falsificación de una firma no es una utopía, por el contrario, es más frecuente de lo que se imagina. Con este tipo de sistemas, la validación de una imitación de una firma genuina se reducirá vertiginosamente gracias al entrenamiento de datos y a la obtención de resultados cada vez más competentes.

- **Necesidad de ahorro en el tiempo de trabajo.** De media, en el sector administrativo, la mitad de la jornada de trabajo de estos empleados se pierde en el tratamiento de documentación en papel o en la entrada de datos. Este problema se verá disminuido gracias a la aceptación de estos sistemas.

- **Necesidad de una reducción de costes (a través de la optimización de procesos operativos).** Debido a la gran cantidad de firmas en documentos, se desperdician recursos como papel, tinta y espacio de almacén.

- **Necesidad de aumentar la eficiencia.** Como en todo proyecto de ingeniería, el primer motivo que impulsa a desarrollarlo, es el hecho de mejorar el rendimiento de procesos ya existentes que, con el tiempo, han ido adquiriendo carencias importantes o no se ajustan al desarrollo tecnológico actual.

Además de estas necesidades, la motivación principal de este proyecto ha sido:

- El estudio y evaluación del rendimiento del sistema al utilizar un smartphone de gama media como dispositivo de captura, realizando la escritura de la firma usando el dedo como útil.

- Observar cómo afecta al rendimiento del sistema el uso del dedo a la hora de realizar la firma frente al uso más tradicional de un lápiz.

- Estudiar el efecto de la interoperabilidad entre los diferentes dispositivos para comprobar si el rendimiento de estos sistemas no se ve gravemente perjudicado.

1.2 Objetivos

Este proyecto desarrollado en el laboratorio del Grupo de Reconocimiento Biométrico ATVS de la Escuela Politécnica Superior de la Universidad Autónoma de Madrid, y en el cual se lleva trabajando algunos años atrás, pretende convertir el uso de la firma, como rasgo biométrico, en una alternativa eficiente en lo que a la identificación de individuos se refiere. Este proyecto estudia las oportunidades que ofrece este concepto en un marco social en el que el gran impacto tecnológico, cada vez más avanzado y competitivo, ha dado lugar a multitud de dispositivos. Mientras que algunos dispositivos como la tableta **WACOM**, se han creado para el uso exclusivo de la captura de **firma digital,** otros como la **tableta Samsung** y **smartphones** de gama media, comienzan a utilizarse como dispositivos de captura de firma dinámica cada vez más frecuentemente. Con el motivo de estudiar más a fondo estos nuevos dispositivos, en este proyecto se ha planteado el uso del smartphone como útil de escritura.

En general, los objetivos son:

1. Captura de la base de datos:

Uno de los objetivos es la captura de la **base de datos e-Biofirma** DS2 (Data Set 2), multisesión (con dos sesiones por cada usuario separadas en el tiempo), multimodal (los usuarios han realizado tanto su firma como procesos de escritura), lo suficientemente grande como para dar resultados fiables y se han utilizado tres **dispositivos**. Estos dispositivos son: una tableta WACOM-STU530, una tableta Samsung Galaxy Note 10.1 y un smartphone Samsung Galaxy SIII Neo, cada uno de ellos con el protocolo de adquisición establecido. En el *Anexo A* se pueden ver las características de cada dispositivo de captura.

En esta misma base de datos cabe destacar el proceso de realización de falsificaciones que se explicará en detalle en la *Sec. 3.2*. La realización de imitaciones se ha hecho mediante dos procesos. Un proceso realista, en el cual los usuarios tenían poca información acerca de la firma genuina, y mediante un proceso no realista, en el cuál estos mismos usuarios tenían mucha más información acerca de la misma. Posteriormente, se ha hecho un análisis del rendimiento del sistema utilizando los distintos tipos de falsificaciones de firmas.

2. Evaluación del rendimiento de un sistema de reconocimiento de firma:

En este proyecto hay una etapa de experimentación que cabe destacar y que será esencial en la toma de decisiones finales. Se puede afirmar que uno de los principales objetivos de este proyecto, es continuar con el estudio y la mejora de los sistemas que tienen como entrada la firma como rasgo biométrico. Para ello, se han simulado distintas situaciones y estudiado cada una de ellas. El principal objetivo en esta parte es evaluar el rendimiento del sistema cuando el usuario firma con el dedo en un smartphone frente a cuando firma con el lápiz en una tableta diseñada para la captura de firmas. También se ha analizado la **interoperabilidad** entre los distintos dispositivos, que se verá cómo influirá en la toma de decisiones.

1.3 Metodología y plan de trabajo

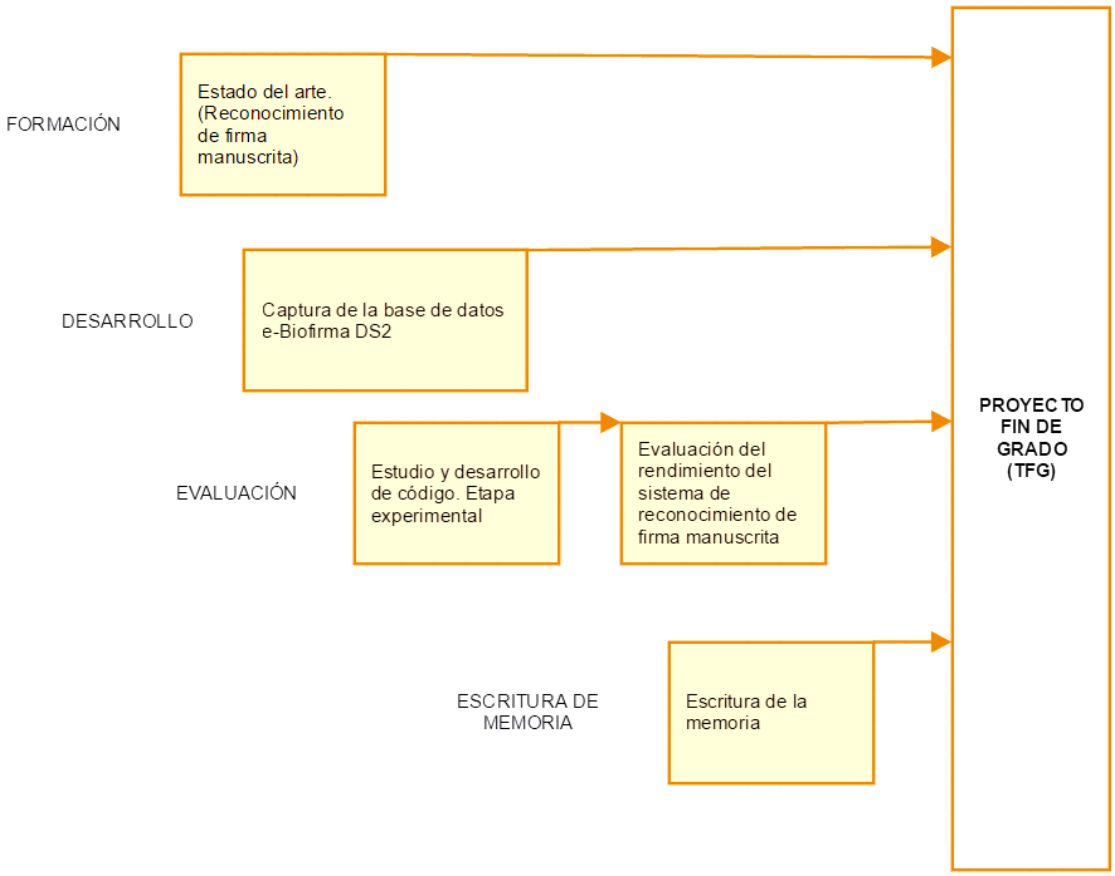


Figura 1: Diagrama del plan de trabajo seguido

En este apartado se va a dar una visión general de cuál ha sido el plan de trabajo del proyecto, el cual se ha llevado a la práctica de la forma más rigurosa posible:

- **Estudio del estado del arte**. Todo inicio de un proyecto pasa por una etapa de formación en la que se obtienen los conocimientos necesarios para su desarrollo. Para este proyecto en concreto, se ha realizado un estudio de los conceptos básicos del **reconocimiento biométrico**, utilizando libros y publicaciones.

- **Desarrollo.** En esta etapa se realiza el diseño y adquisición de la base de datos multi-dispositivo. Previamente, se comprueba que todos los dispositivos disponibles para la adquisición de la base de datos disponen de la aplicación de captura en Java o Java-Android que se desarrolló en proyectos anteriores.

- **Evaluación.** Posteriormente, se han realizado distintos experimentos (mediante la herramienta **Matlab**), con el objetivo de analizar diferentes situaciones y poder comparar posteriormente los resultados con los obtenidos en proyectos anteriores. Además, se ha analizado de qué forma afecta al rendimiento del sistema la firma realizada con dedo en caso de utilizar un smartphone como dispositivo de captura.

Esta etapa junto con la de desarrollo, han sido las más largas en tiempo de proyecto.

- **Escritura de memoria.** Se ha realizado un análisis de los resultados obtenidos en las pruebas llevadas a cabo, así como una comparativa exhaustiva entre los diferentes dispositivos de captura utilizados. Estos análisis, junto con la revisión del estado del arte y un estudio completo del proyecto llevado a cabo, han servido para elaborar la memoria del presente proyecto fin de grado.

2| Estado del arte

2.1 Necesidad de biometría

El término biometría proviene de las palabras 'bio', que significa vida, y 'métrica', que significa medida, por lo tanto, con ello se infiere, que todo sistema biométrico mide e identifica alguna característica propia de la persona. Toda característica única y mesurable (desde la forma de teclear, hasta el olor corporal de una persona), puede considerarse rasgo biométrico, sin embargo, se ha elegido el siguiente esquema para detallar los dos grandes grupos principales de estos rasgos:

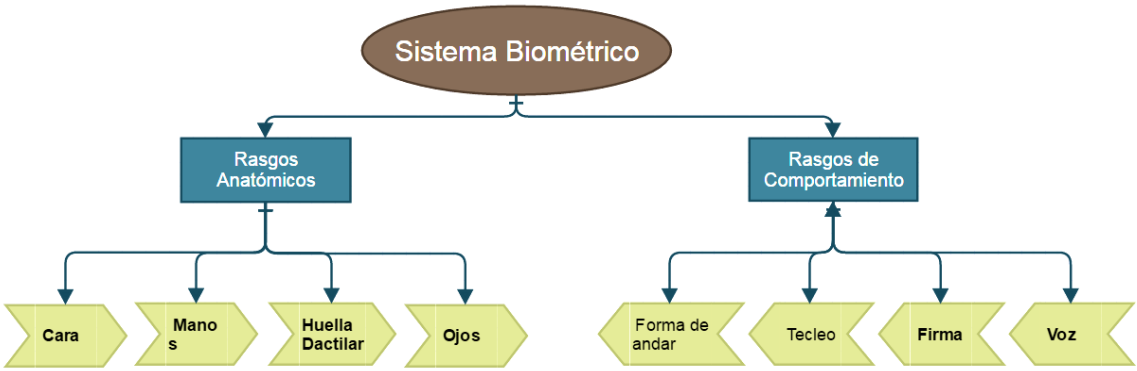


Figura 2: Esquema de los distintos rasgos biométricos

Como se puede observar en la *Fig. 2* a la izquierda, el rostro, manos, huella dactilar e iris o retina, se consideran biometría estática *[3]*. La medición de las características de comportamiento (Véase *Fig.2* derecha*)* es conocida como biometría dinámica. Los principales estudios y aplicaciones de la biometría dinámica están basados en la firma manuscrita y la voz *[7]*.

Cada uno de estos rasgos presenta ventajas e inconvenientes, por lo que no se puede decir que alguno cumpla todos los atributos (que se describen a continuación) de forma exitosa, sin embargo, todos ellos los deben cumplir en mayor o menor medida *[3]*. Los atributos son:

- **Universalidad.** Existencia del rasgo en todos los usuarios
- **Unicidad.** Capacidad discriminativa del rasgo.
- **Permanencia.** El rasgo no varía excesivamente en el tiempo.
- **Mensurabilidad.** El rasgo es mesurable, es decir, puede ser caracterizado cuantitativamente (medido).
- **Aceptabilidad.** Es el grado de aceptación social y personal.
- **Rendimiento.** Precisión y rapidez del sistema
- **Seguridad.** Resistencia que ofrece el sistema a ser burlado.

En general, los sistemas de identificación tradicionales no dan acopio para la creciente demanda de seguridad que solicitan las empresas, cada vez más interesadas en verificar,

con la mayor precisión, la identidad de los individuos que acceden a zonas restringidas o a documentación de carácter confidencial. Por ende, la identificación biométrica está experimentando una mayor aceptación en la sociedad.

2.2 Principales aplicaciones de la biometría

La tecnología de los sistemas que se basan en la **verificación** de la identidad mediante rasgos biométricos, está evolucionando de manera vertiginosa y tiene un fuerte potencial que hace que sea especialmente interesante en determinadas áreas. Entre las múltiples aplicaciones que se tienen para proporcionar seguridad en el reconocimiento de la identidad de la persona, se han querido destacar las siguientes:

- **Banca Electrónica.**

Este es, sin duda, el sector con mayor crecimiento biométrico que se ha experimentado en los últimos años. Y no se habla solo de su uso, ya imprescindible del que se están beneficiando muchas entidades (bancos e instituciones financieras; como VISA o MasterCard), sino también cabe destacar la contribución económica que algunas de ellas aportan a seguir investigando y mejorando estos sistemas. Y es que se puede considerar como el sector históricamente más preocupado por la seguridad, debido a la gran pérdida económica que han experimentado años atrás a causa de los sistemas de reconocimiento tradicionales.

- **Control de acceso físico.**

Uno de los principales motivos que llevan al estudio de sistemas biométricos, es la necesidad de seguridad. El objetivo del reconocimiento biométrico, es asegurar la seguridad haciendo que el individuo sea insustituible y que prácticamente sea imposible que un empleado registre la asistencia de otro. Las puertas blindadas, las rejas en los portales o los torniquetes, son medios de acceso que, en muchos casos, quedarán obsoletos en un futuro.

El funcionamiento que utilizan los sistemas de reconocimiento biométrico es el siguiente: leen una característica o serie de características físicas (estáticas) o de comportamiento de la persona, consideradas suficientes para su identificación (siendo los más usuales la huella dactilar, la forma del iris o los patrones faciales), y la contrastan con muestras correspondientes a ese usuario y contenidas en una base de datos interna de la empresa. El objetivo es corroborar que un individuo es quien asegura ser. Cuando el sistema detecta que está tratando con un autorizado, permite que éste acceda al lugar que se propone. La validación o identificación biométrica es una de las mejores alternativas de seguridad del momento, ya que solo implica una inversión y se requiere poco mantenimiento. Además, la puesta en marcha de un sistema así es simple: se toman los datos de los autorizados y luego el control de acceso biométrico se encarga del resto.

El control de acceso físico, se encuentra implantado en instituciones financieras, organizaciones de salud, centros educativos, oficinas, gimnasios, hogares, clubes, etc. Los aeropuertos son infraestructuras donde el control de acceso cobra gran importancia.

Fue a partir del trágico 11 de Septiembre de 2001, con el atentando de las Torres Gemelas de Estados Unidos, cuando la seguridad aeroportuaria, (tanto física como tecnológica) aumentó. Comenzaron a interesarse por sistemas renovados, fiables, basados en reconocimiento biométrico, los cuáles fueron financiados por programas de iniciativa privadas apoyadas por el gobierno. Sobre todo causó gran interés en los expertos dedicados a la seguridad aeroportuaria que comenzaron a desarrollar aplicaciones en los aeropuertos de todo el mundo, siendo este desarrollo más lento en Europa, dónde la adopción de estos nuevos sistemas solo se empezó a implantar en grandes aeropuertos como el de Schipol-Amsterdam y el de Heathrow-Londres.

En España, la empresa Indra ha desplegado sus sistemas biométricos ABC (Automatic Border Control - Control Automatizado Fronterizo) y lo ha hecho en 7 aeropuertos españoles (Madrid, Barcelona, Girona, Palma de Mallorca, Alicante, Tenerife Sur y Málaga) y en la Estación Marítima de Algeciras en la que todos los años se registra un gran flujo de viajeros que llegan de toda Europa para cruzar hacia África.

Este sistema cuenta con una especie de quiosco en el cual el viajero introduce su DNI electrónico o pasaporte digital, a continuación, se cuenta con varios puestos en los que se recoge la huella dactilar y se procede al reconocimiento facial del individuo. De esta forma, el sistema contrasta los parámetros biométricos del viajero, con la que aporta el documento digital, al tiempo que verifica la autenticidad del mismo y lleva a cabo una consulta a las bases de datos policiales. En dicho proyecto han intervenido tanto Indra como el Cuerpo Nacional de Policía y la Dirección Técnica de la Secretaría de Estado de Seguridad. "Todo este proceso se completa en solo unos pocos segundos y, a continuación, el viajero puede dirigirse hacia la puerta de paso por frontera" ha destacado Indra.

- **Ámbito forense.**

Los sistemas de reconocimiento de la identidad a partir de rasgos biométricos también se utilizan en aplicaciones forenses, tales como investigación criminal, identificación terrorista, análisis de paternidad y desapariciones.

La teoría de unicidad de la huella dactilar, que afirma que no existen dos huellas dactilares iguales, está ampliamente aceptada en todo el mundo.

Con el paso de los años son muchos los avances que se han realizado en el campo de la biometría forense en general. El crecimiento de las bases de datos forenses de huellas dactilares ha hecho que la indexación y la comparación manual de huellas sean cada vez más complicadas. Los avances de la tecnología han permitido la creación de sistemas automáticos de identificación dactilar, conocidos como AFIS.

En general, en el ámbito de la criminalística y en el marco de un proceso jurisdiccional, el proceso de identificación va frecuentemente acompañado de **autenticación**. La autenticación de un sospechoso, tiene como fin último su individualización, es decir, la certeza de distinguir una persona del resto de una población. Este objetivo se logra, como se ha mencionado con anterioridad, gracias a rasgos biométricos como la huella dactilar, pero también la voz. Un sistema de reconocimiento automático de locutor puede realizar la comparación entre una locución cuestionada grabada y una locución de control indubitada tomada de un sospechoso identificado (por ejemplo, grabaciones realizadas en dependencias policiales).

2.3 Sistemas de reconocimiento biométrico

En los sistemas de reconocimiento biométrico existen varios modos de operación. En capítulos anteriores, se ha hablado del concepto de identificación, pues bien, este concepto se trata de un modo de operación dentro de los sistemas de reconocimiento biométrico, pero no es el único, también está el modo verificación *[7]*. Tras el proceso de registro (Véase *Sec. 2.4.3*), el sistema puede entrar en funcionamiento en dos modos diferentes:

En el modo de identificación (Véase *Fig. 3*), en el cuál el sistema recoge el patrón obtenido del individuo y hace una comparación o **matching** 1:N en la base de datos, es decir, se compara la muestra que entra al sistema, con cada una de las muestras que contiene la base de datos. Esto hace que aumente en gran medida el coste computacional del sistema y más aún, cuando se aumenta dicha base de datos.

Finalmente, se obtiene la identidad del usuario o un mensaje de error en caso de que no se encuentre en la base de datos.

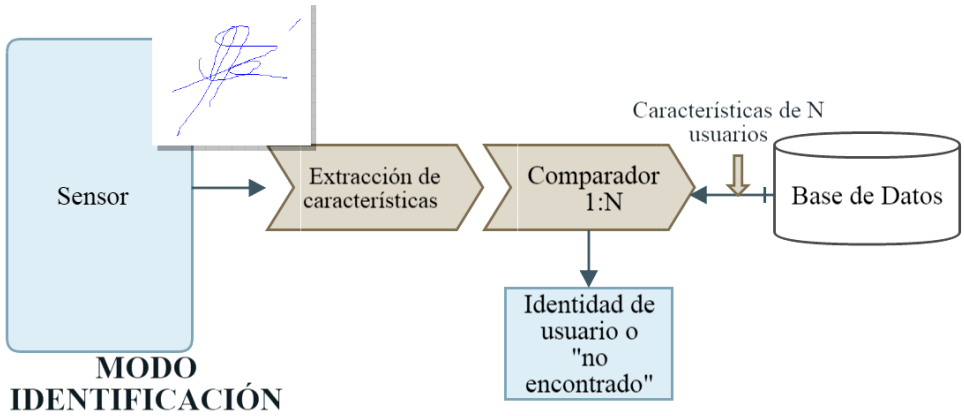


Figura 3: Modos de operación en el reconocimiento biométrico. Modo identificación. Figura adaptada de [8]

En el modo de verificación (Véase *Fig. 4*), el individuo previamente ha insertado un PIN, contraseña o tarjeta identificadora que contiene su identidad. A continuación, el sistema obtiene el rasgo biométrico del usuario y realiza una comparación (matching), esta vez, 1:1, es decir, se compara la muestra de entrada con la muestra que se ha obtenido de la base de datos que coincide con ese pin o contraseña. En este caso, el coste computacional disminuye en gran medida. En este modo, obtendremos una salida positiva en caso de que estos dos rasgos coincidan, o negativa en caso contrario.

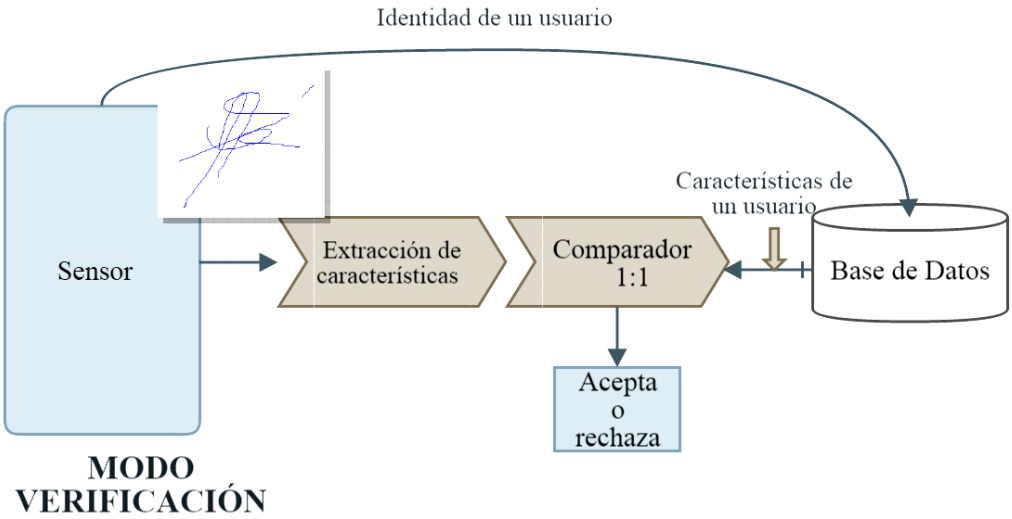


Figura 4: Modos de operación en el reconocimiento biométrico. Modo verificación. Figura adaptada de [8]

2.4 Sistemas de verificación de firma On-Line

Antes de comenzar a explicar la funcionalidad y los detalles de este tipo de sistemas, es necesario explicar el concepto de firma on-line. Se pueden clasificar los métodos de verificación de firma en dos grupos principales:

- On-line: Estos sistemas utilizan características dinámicas para dicha verificación, como pueden ser, la inclinación del bolígrafo, la presión ejercida, la velocidad del trazo, etc. Estos parámetros son recogidos por dispositivos como tabletas digitales (Véase *Fig. 5 (a)*).

- Off-line: En este caso, se va a utilizar la firma estampada en un papel o documento (Véase *Fig. 5 (b)*). Las características se extraen escaneando dicha firma y sacando características geométricas de ella para después, poder verificar la identidad del firmante.

(a) *(b)*

Figura 5: Sistemas de verificación de firma On-line (a), Offline (b)

De estas dos definiciones se puede sacar una conclusión obvia y es que, gracias a la firma on-line, se puede identificar con mayor facilidad a la persona, debido a la gran cantidad de información que aporta. Por lo tanto, se obtendrán mejores resultados frente al uso de la firma off-line en sistemas de verificación.

A continuación, se procede a explicar en detalle las características y procedimientos de la firma manuscrita dinámica ya que es el tipo de firma que se va a estudiar en profundidad. En la *Fig. 6,* se puede observar la arquitectura que presentan este tipo de sistemas. A continuación, se explica cada parte en detalle.

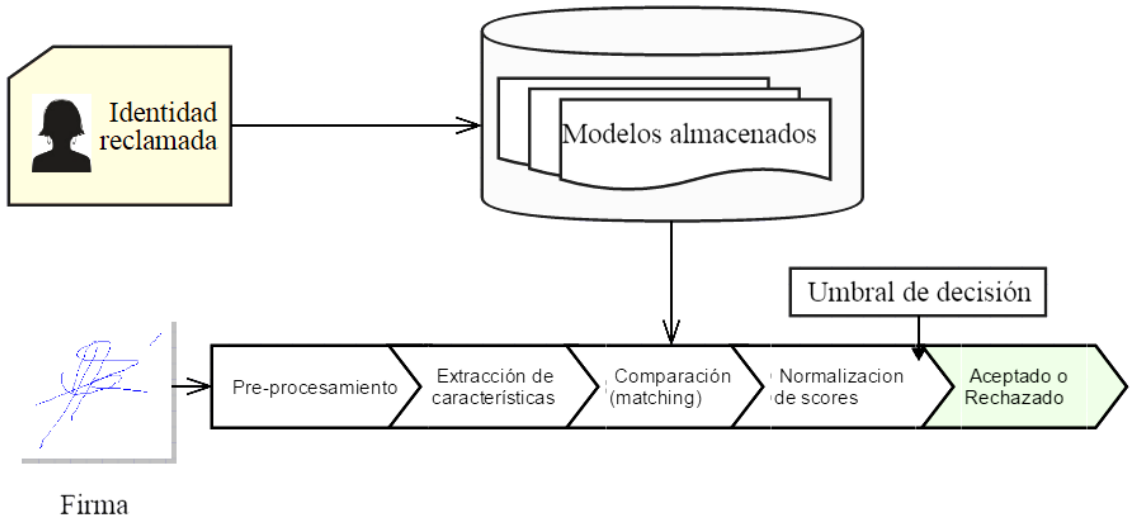


Figura 6: Arquitectura de un sistema de verificación de firma dinámica manuscrita

2.4.1 Captura de datos

Las señales de una firma son capturadas por distintos dispositivos. Dependiendo del dispositivo que se utilice para realizar la captura, se obtendrá más información o menos. Por ejemplo, si se quiere recoger una firma mediante una tableta digital (p.ej. WACOM) se adquirirá mucha información sobre esa firma, como puede ser la presión, la trayectoria del bolígrafo e incluso el ángulo de inclinación del bolígrafo durante el proceso de firmado. Mientras que otros dispositivos no diseñados para captura de firmas, como pueden ser los smartphones de gama media o tabletas Android, no tienen la capacidad de recoger toda esa información.

Por otro lado, la mayor frecuencia observada a la hora de realizar una firma suele ser entre 20-30 Hz *[9]*. Estos dispositivos de captura, muestrean las señales a una frecuencia entre 100-200 Hz, por lo tanto, se cumple con el criterio de Nyquist.

Tras la captura de los datos, se procede a realizar un pre-procesado, que en algunos casos, será distinto dependiendo del dispositivo que se emplee. Generalmente, este pre-procesado se basa en eliminar el ruido mediante un filtrado, aplicar técnicas de diezmado para eliminar posibles muestras repetidas y en ciertos casos, aplicar una interpolación con el

objetivo de que la frecuencia de muestreo sea igual en todos los dispositivos. Es decir, que una firma de un mismo usuario se parezca lo máximo posible en cada uno de los dispositivos.

2.4.2 Extracción de características

Para cada sistema biométrico, interesará obtener unas u otras características, por ejemplo, en un sistema de reconocimiento de la voz se deseará encontrar aquellas tales como los lazos armónicos en las vocales (que dependen solo del hablante y no de las palabras que son habladas). Pero en esta parte, se va a describir la firma como rasgo biométrico.

Va a interesar la extracción de información discriminatoria a partir de los datos de la firma on-line. Y aquí se presentan las dos grandes clases en las que se pueden agrupar los métodos de dicha extracción:

- **Sistemas globales o basados en características globales.** Basados en características globales derivadas de la trayectoria de la firma.

- **Sistemas basados en funciones.** Mediante secuencias de tiempo, estas funciones son capaces de describir propiedades de la firma como su velocidad, presión y trayectoria. Este es el método que se ha utilizado en este proyecto y que se ha visto cómo es capaz de proporcionar mejores resultados que los sistemas basados en características.

Para ver estos dos métodos en mayor detalle, véase *Sec. 2.5*.

2.4.3 Registro

Anteriormente, se han visto los distintos modos de operación y la forma en la que se comparaban las muestras de entrada con las muestras que hay en la base de datos, o dicho de otro modo, la estrategia de comparación o matching.

Esta sesión de registro es supervisada y en ella se comprueba manualmente la identificación del usuario, para ello se utilizan de 4 a 6 firmas.

2.4.4 Similitud (pre-alineamiento y matching)

Con el objetivo de mejorar el rendimiento, en esta etapa, se suele hacer un pre-alineamiento de las muestras de la firma del usuario entrante y las muestras almacenadas correspondientes con el modelo de ese usuario. Tras este proceso, se realiza el de comparación (matching). En los sistemas globales o basados en características, se suele utilizar técnicas basadas en la medida de distancias. Entre algunos ejemplos que cabe destacar se encuentran: la distancia Euclidea o la de Mahalonobis *[10]*. Por otro lado, los

sistemas locales o basados en funciones temporales utilizan otro tipo de técnicas (Véase *Sec. 2.5.2*).

2.4.5 Normalización de scores

Los scores o puntuaciones se normalizan según un modelo usado para que todos estos puedan ser tratados con el mismo criterio. Por ejemplo, en este caso, las puntuaciones obtenidas tras las comparaciones de la muestra de entrada con las muestras registradas, son normalizadas a un rango común [0,1]. Estas transformaciones tienen que ser lineales, crecientes o decrecientes. Se debe aplicar esta misma transformación a todos los scores, tanto a los obtenidos en comparaciones genuinas como en comparaciones impostoras, para que su tratado posterior sea ecuánime. Este proceso es de gran importancia en los casos en los que se utilicen técnicas de fusión de sistemas.

2.5 Extracción de características. Sistemas globales y locales

En este punto, se va a profundizar en la extracción de características.

2.5.1 Sistemas globales

Este tipo de sistemas se basan en crear un vector de características extraídas de la firma. Estas características pueden ser el número de pen-ups, la velocidad promedio de la firma, la duración, etc. Sin embargo, como ya se ha citado anteriormente, únicamente se disponen de cuatro firmas genuinas de entrenamiento, por lo que el número de características que se han introducido en el vector, ha sido menor a la hora de implementar el sistema de este proyecto. Para seleccionar las características que finalmente se han utilizado, se ha usado el algoritmo SFFS como técnica de selección de características, ya que proporciona mejores resultados, a costa de un mayor coste computacional.

2.5.2 Sistemas locales

En este caso, se obtienen características como la presión, coordenadas, etc. Estas características son funciones capturadas en el tiempo y son utilizadas para modelar la firma de cada usuario.

Cabe destacar que la fusión de los sistemas globales (basados en características) y los sistemas locales (basados en funciones) proporcionan un mejor rendimiento que considerando cada uno de los sistemas por separado *[11]*.

Las técnicas más utilizadas en este tipo de sistemas son HMM (Hiden Markov Models) y DTW (Dynamic Time Warping). Este proyecto se ha centrado en DTW ya que es el que se ha utilizado para la implementación del sistema. Por otro lado, HMM es una técnica muy utilizada en biometría, pero sobre todo, en reconocimiento de voz, aunque en el ámbito de verificación de firma manuscrita dinámica también se han utilizado diferentes aproximaciones de este algoritmo, que se pueden ver en *[15][16]*.

2.5.3 Dynamic Time Warping

El alineamiento temporal dinámico (Dynamic Time Warping, DTW) *[12]*, es una técnica que permite comparar dos secuencias temporales de distinta longitud.

Este algoritmo surge de la problemática de la inexistencia de una sincronización temporal (alineamiento temporal) entre dos patrones. Además, esta falta de alineamiento no obedece a una ley fija (p.ej. un retardo constante), sino que se da de forma heterogénea, produciéndose así, variaciones localizadas que aumentan o disminuyen la duración del tramo de análisis. Por lo que será necesario alinear temporalmente los patrones para proceder a realizar una medida de distancia entre ellos cuyo nuevo eje temporal haya homogeneizado las variaciones iniciales.

Alineamiento temporal (temporal warping). En este proceso, el eje temporal de la señal de test se comprime y expande de forma no lineal para alinear los vectores de características entre patrón y test. Resultado del proceso de alineamiento surge el concepto de camino de alineamiento.

De forma genérica, se puede presentar la función de alineamiento a través de una representación del tipo siguiente (Véase *Fig. 7*).

Si observamos la función de alineamiento en detalle, tendremos que:

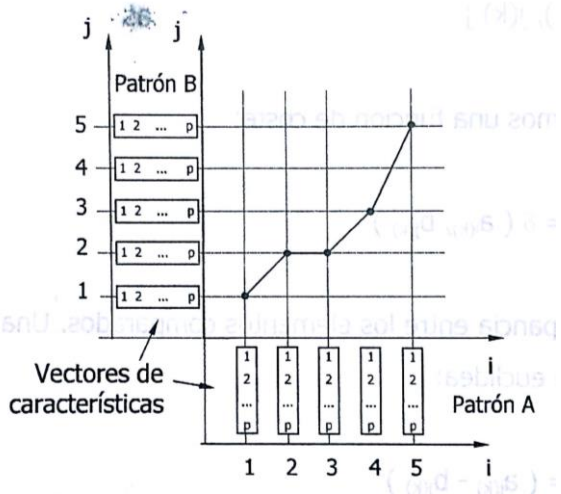


Figura 7: Ejemplo de la función de alineamiento en detalle

Si la función de alineamiento pasa por (i, j), comparamos el vector 'i' del patrón A con la 'j' del patrón B.

El problema, por lo tanto, consistirá en encontrar la función de alineamiento a partir de dos vectores de características (patrones) 'A' y 'B':

$$A = \{a_1, a_2, .., a_i, .., a_M\} \quad (3.1)$$

$$B = \{b_1, b_2, .., b_i, .., b_M\} \quad (3.2)$$

Y una medida de distancia:

$$d(i,j) = \|x_i - y_j\| \qquad (3.3)$$

Llamando 'C' a la función de alineamiento que puede ser definida como:

$$C = c_1, c_2, \ldots, c_k, \ldots, c_K \qquad (3.4)$$

Donde cada c_k representa una correspondencia (i,j) entre las muestras de las secuencias A y B. La condición general del algoritmo es la siguiente:

$$g_1 = g(1,1) = d(1,1)\,.w(1) \qquad (3.5)$$

Donde g_k representa la distancia acumulada después de *k* pasos y w_k es un factor de ponderación que deber ser definido. Para cada iteración, g_k es calculado como:

$$g_k = g(i,j) = min_{c_{k-1}}[g_{k-1} + d(c_k)\,.w(k)\,] \qquad (3.6)$$

Hasta alcanzar la muestra final I y J de ambas secuencias. La distancia acumulada final es normalizada.

El factor w_k se define con el objetivo de restringir la correspondencia entre muestras de ambas secuencias. Con la definición de *Ecu 3.6* se obtiene:

$$g_k = g(i,j) = min\begin{pmatrix} g(i,j-1) + d(i,j) \\ g(i-1,j-1) + 2d(i,j) \\ g(i-1,j) + d(i,j) \end{pmatrix} \qquad (3.7)$$

Esta es una de las implementaciones más comunes. A continuación, en la *Fig. 8*, se va a mostrar un ejemplo de la correspondencia punto a punto entre dos muestras de firmas genuinas donde se pueden observar los resultados de alineamiento temporal.

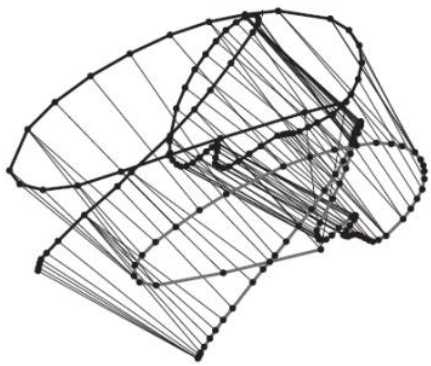


Figura 8: Ejemplo de la correspondencia punto a punto usando DTW entre dos secuencias de firmas genuinas [13]

3| Base de datos e-Biofirma DS2

Una base de datos es un sistema informático a modo de almacén. Este almacén contiene grandes volúmenes de información. Toda base de datos debe tener una serie de características tales como seguridad (sólo personas autorizadas podrán acceder a la información), integridad (la información se mantendrá sin pérdidas de datos), e independencia (esta característica es fundamental ya que una buena base de datos debería ser independiente del sistema operativo o programas que interactúen con ella). Hay más características que debe reunir una base de datos, como ser consistente (es decir, que la información se guarde sin duplicidades y de manera correcta).

Hace unos años atrás, se creaban y utilizaban bases de datos multimodales (base de datos que contiene muestras capturadas por diversos dispositivos) a partir de mezclas de bases de datos unimodales. Sin embargo, estos datos no estaban correlados, puesto que la adquisición no había seguido el mismo protocolo de captura, por lo que los resultados no eran del todo reales. Los sistemas biométricos multimodales reales, son aquellos que capturan los distintos rasgos biométricos de la persona a través de múltiples sensores. Estos sistemas resultan más confiables debido a la presencia de múltiples porciones de evidencia; asimismo, estos sistemas tienen la capacidad de satisfacer los requerimientos severos de desempeño impuestos por algunas aplicaciones.

Debido a la necesidad que había de crear bases de datos multimodales reales y eliminar las falsas existentes, surgieron bases de datos tales como MCYT (2003), BIOMET (2003), BioSec (2007), BiosecurID (2007) o Biosecure (2008). Estas bases de datos ofrecen tanto ventajas como inconvenientes. Uno de los principales inconvenientes, ha sido el aumento de tiempo que conlleva la creación de estas bases de datos, que justifica la escasa existencia de éstas.

A continuación, se van a detallar las características de algunas de las bases de datos anteriores en las que el Grupo de Reconocimiento Biométrico, ATVS, de la Universidad Autónoma de Madrid (UAM), ha intervenido:

- MCYT: La adquisición de esta base de datos se caracteriza por incorporar firmas y huellas dactilares de 330 individuos. Con respecto a las huellas dactilares, se recogieron doce muestras de cada uno de los dedos mediante dos sensores diferentes. Y con respecto a la firma, se registraron 25 firmas genuinas y 25 falsificadas. Estas firmas incluyen tanto información on-line como off-line.

- BiosecurID: Esta base de datos es un proyecto fundado por el Ministerio de Ciencia y Tecnología en el que han participado seis instituciones españolas entre las cuales se encuentra el grupo de ATVS. El principal objetivo de esta base de datos es construir una nueva base de datos multimodal extendiendo la ya existente BIOSEC, es decir, incluir nuevas sesiones para sujetos ya registrados, así como incluir nuevos datos biométricos y nuevos sujetos. Los rasgos biométricos de los cuales consta esta base de datos son: Imagen facial 2D, geometría de la mano, huella dactilar, escritura, iris, dinámica de tecleo, firma y voz. El número de usuarios ya registrados aumenta hasta 400.

- Biosecure: En este proyecto han participado más de 30 instituciones de investigación procedentes de 15 países. El grupo ATVS se encuentra a cargo de las actividades relacionadas con la adquisición de muestras a través de Internet. Esta base de datos incorpora tres conjuntos: Internet, escritorio y móvil. Esta base de datos se caracteriza por incorporar dos dispositivos en la captura de datos como son la WACOM y PDA.

3.1 Diseño y descripción

En esta sección se va a describir el diseño para la base de datos e-Biofirma DS2.

Primero se va a describir el entorno físico en el que se realizó la adquisición de las muestras. Esta base de datos se realizó en dos entornos principales, uno de ellos fue el CAU (Centro de Atención a Usuarios) de la Universidad Autónoma de Madrid ubicado en el edificio B de la EPS (Escuela Politécnica Superior). Y el otro fue una clase de programación de primero de Grado en Tecnologías y Servicios de Telecomunicación, también situada en la EPS. Se esperaba que el primer grupo formado por trabajadores del CAU contase con 80 usuarios, mientras que el grupo de estudiantes contase con 20 usuarios. Finalmente, debido a una serie de problemas que surgieron (Véase *Anexo B*), la base de datos cuenta con 53 usuarios en total (Véanse las proporciones en la *Tabla 2*).

Los motivos principales de realizar esta captura en estos determinados entornos fueron las siguientes:

- Poder ampliar esta base de datos en un futuro y poder observar la evolución de la firma (como rasgo biométrico) en el tiempo. Este último motivo ha sido el principal que ha impulsado a que los participantes fuesen estudiantes de primeros cursos o trabajadores de la universidad, ya que se espera que permanezcan en la universidad tres años más como mínimo.

- Poder captar a usuarios de manera sencilla, estableciendo a la persona responsable de ofrecer ayuda a los participantes en un puesto fijo y facilitarles, de la misma forma, el poder acudir nuevamente a las posteriores sesiones que se han realizado.

- Imitar el proceso de captura de la manera más realista posible.

El espacio de captura se puede observar en la *Fig. 9*. Una vez que se comprobó que todos los dispositivos disponían de la aplicación de captura (desarrollada en el proyecto de "Diseño y adquisición multi-dispositivo de base de datos de firma manuscrita dinámica", por Sandra Gaytán en julio del 2014), se pasó a la captura de los datos. Se tomó la decisión de ensayar el método de adquisición con compañeros del laboratorio de ATVS, para evitar posibles errores y actuar a tiempo, antes de comenzar la captura definitiva para la base de datos.

Los usuarios que pasaban por el puesto, procedían a realizar el proceso de firma y escritura en cada uno de los dispositivos, firmando previamente un consentimiento.

Figura 9: Entorno físico de captura de firmas con todos los dispositivos que han intervenido

Los tres dispositivos que han intervenido en esta base de datos han sido una tableta WACOM-STU530, una tableta Samsung Galaxy Note 10.1 y un Smartphone Samsung Galaxy Neo SIII, para ver en mayor detalle las características de cada uno véase *Anexo A.*

La captura se realizó con los tres dispositivos mencionados anteriormente (Veáse *Fig. 9*), y en dos sesiones, separadas en el tiempo mínimo 15 días entre la primera y la segunda sesión. En cada sesión había dos bloques para cada usuario, que se explicarán en detalle más adelante. La duración de cada sesión ha sido de unos 10 minutos, aproximadamente, para cada usuario.

Esta base de datos se caracteriza por la recogida de tres rasgos biométricos; firma, información de escritura e información de DNI.

- En la WACOM (tableta digital), se firma con el lápiz (stylus o pen) y se escribe el nombre y primer apellido tanto en minúsculas como en mayúsculas. El motivo de la escritura dl nombre y apellido, tiene su razón de ser en el hecho de poder verificar de manera óptima la identidad del usuario, siendo insuficiente la firma de éste.

- En la tableta Samsung Galaxy Note 10.1, que permite tanto captura con pen como con dedo, se firma y se escribe el nombre en mayúsculas y en minúsculas con pen. Posteriormente, firman y escriben números del 0 al 9 con una letra en mayúsculas de las 23 posibles, en este caso, con el dedo. Esto imita el DNI de cada usuario sin necesidad de que introduzcan el suyo oficial ya que, en proyectos anteriores, se decidió hacerlo de esta forma por motivos de privacidad.

- Por último, el teléfono móvil Samsung Galaxy Neo SIII permite la firma y escritura de la secuencia alfanumérica únicamente con el dedo. Retos propuestos en proyectos anteriores, como la adaptación de estos sistemas a dispositivos móviles, cuyo espacio de firma es limitado, se ha logrado con éxito.

En esta base de datos también se han realizado falsificaciones tanto de firma como de escritura (en este proceso no se ha incluido la escritura de números, para no aumentar el tiempo del proceso de captura). Cada usuario se esperaba que falsificase tanto la firma como la escritura de los tres usuarios anteriores a él (según el orden de captura de la base de datos). Finalmente, fueron compañeros del laboratorio de ATVS los que intervinieron en este proceso. Este proceso de realización de falsificaciones se detallará en profundidad en la *Sec. 3.2*.

En la base de datos e-Biofirma DS2, las muestras recogidas con el pen, se almacenan en ficheros '.txt' con la siguiente nomenclatura:

```
U[uid]_s[sid]_g[group]_b[bloque]_[info]_[tool]_[mode]_u[num].txt
```

Dónde:

- **uid.** Número de identificación de usuario.
- **sid.** Número de sesión.
- **group.** Número de grupo (No se usará. Por defecto tendrá valor '1')
- **bloque.** Número de bloque.
- **info.** sign (firma), nam1 (nombre y primer apellido) o nam2 (NOMBRE y PRIMER APELLIDO).
- **tool.** Tipo de dispositivo: w2 (WACOM STU-530).
- **mode.** c (cliente), s (impostor).
- **num.** Número de muestra recogida o, en caso de ser una muestra impostora, se trata del número de identificación del usuario que realiza esa falsificación.

Cada archivo '.txt' contiene la siguiente información relativa a cada firma o nombre recogido:

- Primera fila: número de muestras que compone la firma, nombre o secuencia alfanumérica.

- Resto de filas:

    - Primera y segunda columna: Puntos 'x' e 'y'.
    - Tercera columna: Tiempo.
    - Cuarta columna: Presión.

Cabe destacar que el tiempo de captura se corresponde con el tiempo de la tableta (constante, 5ms entre muestras consecutivas) para la WACOM-530, y con el tiempo del sistema para la Samsung Galaxy Note 10.1, debido a que, esta última, al no ser un dispositivo específico de captura de escritura, no permite obtener el tiempo de la tableta.

Con respecto a las muestras recogidas con el dedo (capturadas con la tableta Samsung Galaxy Note 10.1 y el teléfono móvil Samsung Galaxy SIII Neo), la nomenclatura es muy similar con la excepción de:

- **info.** sFin (firma con el dedo), nFin (DNI con el dedo).

- **tool.** Tipo de dispositivo: w5 (Samsung Galaxy Note 10.1)/ w6 (Samsung Galaxy Neo SIII).

La información que contiene cada archivo '.txt', en este caso de muestras recogidas con dedo, es muy similar a la que recogemos con el pen (Véanse *Fig. 10* y *Fig. 11*).

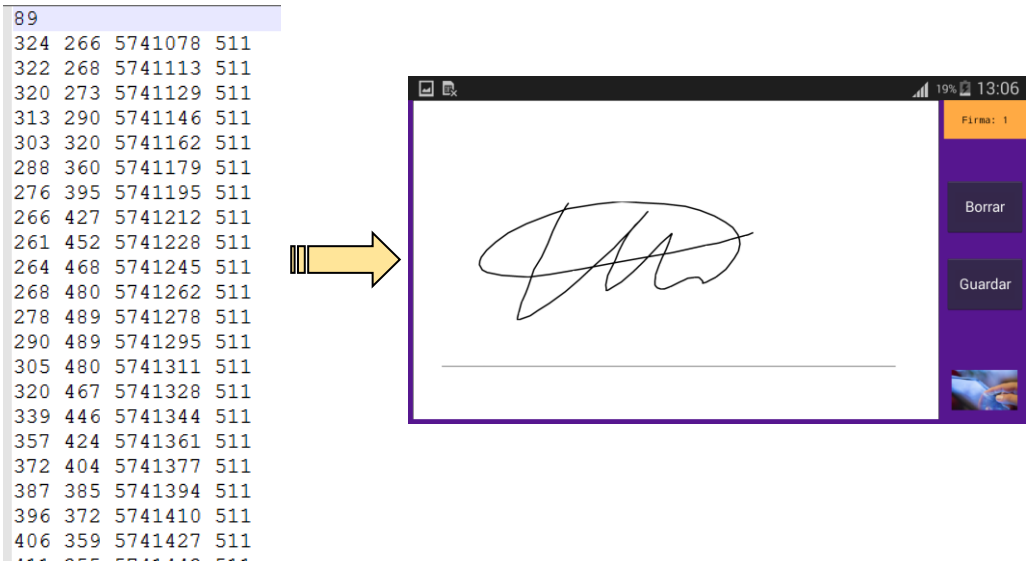


Figura 10: Firma real del usuario 105 realizada con el dedo y capturada con el móvil Samsung Galaxy SIII Neo

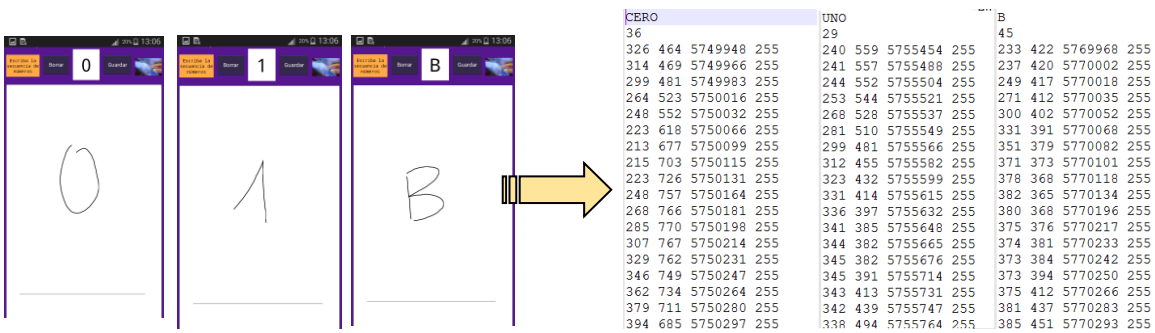


Figura 11: Secuencia alfanumérica real del usuario 105 realizada con el dedo y capturada con el móvil Samsung Galaxy SIII Neo

Viendo las *Fig. 10* y *11*, podemos destacar las siguientes características:

Observamos cómo estos archivos, que contienen muestras realizadas con el dedo, poseen la misma información que las muestras recogidas con pen. En el caso de la secuencia alfanumérica, la información se organiza en las mismas columnas pero con la presencia del número escrito con letra en la parte superior del archivo de texto, al igual que la última letra de la secuencia alfanumérica.

3.2 Proceso de captura / Adquisición de datos

Previamente al proceso de adquisición, se realizó una tabla Excel para rellenar con los datos de cada usuario, con el objetivo de identificarles y poder contactar con ellos vía e-mail para una segunda y última sesión. Estos datos se han recogido en una tabla Excel. En esta tabla se incluyen los siguientes datos:

- **ID.** Identificador único del usuario.
- **Nombre**
- **Apellido**
- **E-mail**
- **S1-fecha.** Fecha de la primera sesión. Este campo se ha incluido con el fin de poder saber con exactitud el momento de empezar a realizar la segunda sesión, comprobando así, los días que han transcurrido entre una sesión y otra.
- **F.** Este campo se selecciona cuando las falsificaciones ya han sido realizadas. Este campo está presente tanto para la primera, como para la segunda sesión.
- **Falsificadores 1sesión.** Nombre y Apellido de la persona que ha hecho el papel de falsificador de dicho usuario. Se recuerda que las falsificaciones no pudieron ser realizadas por los participantes, sino por compañeros del ATVS. Se necesitaba llevar un control para que los falsificadores no repitiesen a los usuarios a los que imita.
- **S2 fecha.** Fecha de la segunda sesión.
- **Curso.** Este campo se rellenaba únicamente cuando el usuario era estudiante. Se ha incluido con el objetivo de saber, aproximadamente, cuántos años más permanecerá en la universidad, para contar con él/ella en posteriores sesiones. (Véase *Sec. 5.2*)
- **Trabajadores UAM.** Este campo se selecciona en el caso de que los participantes de la base de datos sean trabajadores fijos de la universidad.
- **Año.** En este campo se obtiene la edad del participante.
- **D/ Z.** D (Diestro)/ Z (Zurdo).

El proceso de adquisición, ordenado temporalmente, queda esquematizado en la *Tabla 1*. Un usuario que realice este proceso, habrá completado una sesión de captura de la base de datos.

<table>
<tr><td colspan="5">Sesión de captura</td></tr>
<tr><td rowspan="2">PEN</td><td colspan="2">Muestras genuinas</td><td colspan="2">Falsificaciones</td></tr>
<tr><td>Primer bloque</td><td>Segundo bloque</td><td colspan="2" rowspan="2">Firma de los 3 usuarios anteriores:
(x2 dispositivos)
+
Nombre en minúsculas y MAYÚSCULAS de los 3 usuarios anteriores:
(únicamente en w2)</td></tr>
<tr><td>Firma
+
Firma
+
nombre
(x2 dispositivos)</td><td>Firma
+
Firma
+
NOMBRE
(x2 dispositivos)</td></tr>
<tr><td rowspan="2">DEDO</td><td rowspan="2">Firma
+
Secuencia alfanumérica
+
Firma
+
Secuencia alfanumérica

(x2 dispositivos)</td><td rowspan="2">Firma
+
Secuencia alfanumérica
+
Firma
+
Secuencia alfanumérica

(x2 dispositivos)</td><td>Primer bloque
(Proceso no realista)</td><td>Segundo Bloque
(Proceso realista)</td></tr>
<tr><td>Firma de los 3 usuarios anteriores:
(x2 dispositivos)</td><td>Firma de los 3 usuarios anteriores:
(x2 dispositivos)</td></tr>
</table>

1: Proceso generalizado de adquisición de la base de datos e-Biofirma DS2

Tras haber realizado las firmas genuinas y las secuencias alfanuméricas de ambos bloques, se realizan las falsificaciones. En las falsificaciones capturadas con pen de la primera sesión, los usuarios tienen la posibilidad de ver la dinámica de la firma a tiempo y velocidad real de realización, tantas veces como quieran. Mientras que en la segunda sesión, se ha establecido un proceso de falsificación con calco, proporcionando la firma impresa en papel del usuario original, de forma que el falsificador pueda colocarla sobre la pantalla del dispositivo e intentar imitarla. Este proceso se realiza siempre y cuando se estén utilizando como dispositivos de captura aquellos que utilizan pen (Tableta Samsung y WACOM). En este caso, la firma falsificada es muy similar a la genuina, y las principales diferencias se encuentran en la velocidad y presión.

En el caso de las muestras falsificadas recogidas con el dedo, se diferencian dos bloques.

En el primer bloque de la primera sesión, los usuarios tenían la posibilidad de ver la dinámica de la firma genuina. Mientras que en el primer bloque de la segunda sesión, los usuarios tienen delante un papel impreso con la firma genuina e intentan imitar la firma. Tanto en la primera sesión como en la segunda, este bloque no sigue un proceso realista.

Sin embargo, se hizo especial hincapié en el segundo bloque de falsificaciones, el cual se divide en los siguientes pasos:

- **Primer paso.** Como en los casos anteriores de falsificación, el impostor procede a imitar la firma de tres usuarios de la base de datos e-Biofirma DS2. Para realizar dicha imitación, los usuarios tienen la posibilidad de visualizar la firma genuina impresa en un papel unos 30 segundos aproximadamente, en este tiempo, deben

prestar atención al mayor número de detalles para, posteriormente, imitarla lo mejor posible. Este si se considera un caso realista.

- **Segundo paso.** Se identifica al usuario, tanto en la tableta Samsung como en el teléfono móvil, mediante el proceso manual (desarrollado en proyectos previos), ya que solo interesa recoger la firma, y no las secuencias alfanuméricas.

    - Proceso manual *[1]*: Se programó un apartado manual de almacenamiento de muestras que permite reemplazar/almacenar una nueva muestra concreta sin tener que realizar todo el proceso automático. Esta muestra procederá a sustituir la muestra anterior.

La decisión de incluir este proceso realista de falsificaciones, se ha tomado debido a que se ha considerado que las falsificaciones anteriores, tanto en la que el usuario tenía la posibilidad de ver la dinámica de la firma, como en la que simplemente calcaban la firma tras un papel impreso, son situaciones que se alejan bastante de la realidad. Rara vez un impostor va a poseer ese tipo de información acerca de la firma, sin embargo, es más probable que dicho impostor pueda ver la firma estática en algún documento por un corto periodo de tiempo.

Finalmente, los usuarios realizan la segunda sesión, similar a esta primera, con excepción de los puntos que ya se han comentado.

Para llevar a cabo esta adquisición, se desarrollaron (en proyectos anteriores) tres aplicaciones, una para cada dispositivo, en los lenguajes Java (tableta WACOM) y Java Android (smartphone y la tableta Samsung). Siendo tres aplicaciones diferentes, el funcionamiento final de los dispositivos es igual, siguiendo exactamente el mismo protocolo de adquisición.

Los pasos que se realizaron para la adquisición de las muestras de la base de datos e-Biofirma DS2 se pueden ver detalladamente en *[1]*, donde se muestra el proceso de captura con la tableta Samsung, por ser el dispositivo más completo.

Las muestras finales pasan por tres procesos principales:

1. Registro o identificación del usuario
2. Captura de muestras
3. Almacenamiento de las muestras recogidas

Los archivos se almacenan en el directorio correspondiente con la nomenclatura que se ha descrito en la *Sec. 3.1*. En el caso de la tableta WACOM, estos archivos se almacenan en el ordenador, mientras que en los otros dos restantes, las muestras se almacenan en los propios dispositivos.

A modo de resumen, se puede observar en la *Tabla 2*, el número de muestras totales que quedarán almacenadas en la base de datos e-Biofirma DS2 para cada usuario registrado.

- Firmas genuinas: 3 dispositivos x 2 sesiones x 2 bloques por sesión x 2 firmas por bloque = 24 firmas.

- Nombres (minúsculas y mayúsculas): 2 dispositivos x 2 sesiones x 2 bloques por sesión x 1 nombre por bloque = 8 nombres.

- Secuencias alfanuméricas: 2 dispositivos x 2 sesiones x 2 bloques por sesión x 2 secuencias por bloque = 16 secuencias.

- Firmas no genuinas (pen): 2 dispositivos x 2 sesiones x 2 bloques por sesión x 3 firmas por bloque = 24 firmas falsificadas por 3 usuarios diferentes.

- Firmas no genuinas (dedo): 2 dispositivos x 2 sesiones x 2 bloques por cada sesión x 3 firmas por bloque = 24 firmas no genuinas por 3 usuarios diferentes.

- Nombres no genuinos (minúsculas y mayúsculas): 1 dispositivo (WACOM STU-530) x 2 sesiones x 2 bloque por sesión x 6 nombres por bloque = 24 nombres falsificados.

Esto resulta en un total de 48 muestras genuinas + 72 imitaciones = **120 muestras** por usuario.

Dispositivos	3
Modalidad de firma	Pen + dedo
Sesiones por dispositivo	2
Bloques por sesión	2
Firmas genuinas por bloque	4
Nombres genuinos por bloque	1
Secuencias alfanuméricas por bloque	2
Firmas falsificadas por bloque	3 (3 usuarios, una por cada usuario)
Nombres falsificados por bloque	6 (3 usuarios, dos por cada usuario (minus. y MAYUS.) y solo en STU-530)
TOTAL (por usuario)	**120 muestras**

2: Base de datos e-Biofirma DS2

En esta base de datos han participado 53 usuarios de los cuales (Véase *Tabla 3*):

	Porcentajes
Mujeres	41.51%
Hombres	58.49%
Zurdos	3.77%
Diestros	96.23%
Estudiantes de la UAM	35.85%
Trabajadores de la UAM	64.15%
Rango de edad [18-30]	49%
Rango de edad [30-50]	26.42%
Rango de edad [más de 50]	24.58%

3: Porcentaje de los participantes de la base de datos e-Biofirma DS2

4| Desarrollo experimental

En este capítulo, se hace un estudio acerca del rendimiento del sistema en distintas situaciones y con distintos dispositivos, finalmente, se muestran las conclusiones extraídas a partir de este análisis.

Estos experimentos se han obtenido a partir del estudio y análisis de las muestras contenidas en la base de datos e-Biofirma DS2, mediante la herramienta Matlab (herramienta de software matemático que ofrece un entorno de desarrollo integrado (IDE) con un lenguaje de programación propio).

4.1 Sistema de Reconocimiento Biométrico.

El sistema local utilizado en este proyecto está basado en el algoritmo DTW. El motivo por el cual se usa este algoritmo es debido al bajo coste computacional y a la pequeña cantidad de datos de entrenamiento que se posee en un caso común de verificación de firma.

#	Feature
1	x-coordinate: x_n
2	y-coordinate: y_n
3	Pen-pressure: z_n
4	Path-tangent angle: θ_n
5	Path velocity magnitude: v_n
6	Log curvature radius: ρ_n
7	Total acceleration magnitude: a_n
8-14	First-order derivate of features 1-7: $\dot{x_n}, \dot{y_n}, \dot{z_n}, \dot{\theta_n}, \dot{v_n}, \dot{\rho_n}, \dot{a_n}$
15-16	Second-order derivate of features 1-2: $\ddot{x_n}, \ddot{y_n}$
17	Ratio of the minimum over the maximum speed over a 5-samples window: v_n^r
18-19	Angle of consecutive samples and first order difference: $\alpha_n, \dot{\alpha_n}$
20	Sine: s_n
21	Cosine: c_n
22	Stroke length to width ratio over a 5-samples window: r_n^5
23	Stroke length to width ratio over a 7-samples window: r_n^7

Figura 12: Set de características locales utilizado en el presente proyecto

Se puede observar en la *Fig. 13* el set de características. A partir de las coordenada ‘x’, ‘y’ y de la presión de una firma se han podido obtener el resto de características.

4.2 Protocolo experimental.

En el desarrollo experimental solo se van a analizar las firmas, es decir, las muestras obtenidas a partir de los procesos de escritura, como los nombres y las secuencias alfanuméricas, no se tendrán en cuenta en esta sección.

En la base de datos e-Biofirma DS2, se cuenta con un total de 4 firmas genuinas por sesión, por cada usuario y dispositivo. En el caso de las falsificaciones, son 6 firmas por sesión y por dispositivo.

Las firmas de referencia de la etapa de registro son **entrenadas** con las 4 primeras firmas genuinas de la primera sesión. Las 4 firmas genuinas restantes de la segunda sesión, más las 6 falsificaciones, son utilizadas para realizar el **testeo**.

Por otro lado, se van a utilizar dos formas de proceder:

- 1 vs 1: La comparación se hará 1 a 1, una muestra de test con cada una de las muestras de entrenamiento.

- 1 vs 4: La comparación se hará 1 a 4, una muestra de test con las 4 muestras de entrenamiento, obteniendo un solo score como la media de esas 4 comparaciones.

En la *Sec. 4.3.2*, se compararán ambos métodos y se decidirá cuál de ellos mejora el rendimiento del sistema.

A lo largo de los experimentos, se utilizarán dos conceptos que se explican a continuación:

- Scores en el caso random forgeries: es el caso en el que un usuario utiliza su propia firma para hacerse pasar por otro usuario del sistema, es decir, los scores se obtienen comparando esta firma genuina entrante con una firma genuina del resto de usuarios del sistema (52 firmas).

- Scores en el caso skilled forgeries: en este caso los scores se obtienen comparando la firma genuina de un usuario, con todas sus falsificaciones, 6 firmas en este caso.

A continuación se muestra el número de scores que se obtiene de cada proceso:

Caso skilled	Scores genuine	1vs1	4 (test) x 4 (train) x 53 (usuarios) = 848
		1vs4	4 (test) x 1 (train) x 53 (usuarios) = 212
	Scores forgery	1vs1	6 (test) x 4 (train) x 53 (usuarios) = 1272
		1vs4	6 (test) x 1 (train) x 53 (usuarios) = 318
Caso Random	Scores genuine	1vs1	4 (test) x 4 (train) x 53 (usuarios) = 848
		1vs4	4 (test) x 1 (train) x 53 (usuarios) = 212
	Scores forgery	1vs1	52 (test) x 4 (train) x 53 (usuarios) = 11024
		1vs4	52 (test) x 1 (train) x 53 (usuarios) = 2756

4: Cálculo de scores en el caso skilled y random

El comportamiento del sistema se ha estudiado en términos de EER (Equal Error Rate). El Equal Error Rate es una estadística que muestra el rendimiento general del sistema; por lo general, durante la tarea de verificación. La tasa EER es la ubicación en una curva DET (tipo de curvas muy utilizadas en el ámbito del Reconocimiento Biométrico), donde la tasa de falsa aceptación (se acepta una falsificación como firma genuina) y la tasa de falso rechazo (se rechaza una firma genuina por considerarse falsificación), son iguales. Esto se observa en la *Fig. 14*, y de esta forma es como se presentarán, a partir de ahora, las curvas DET.

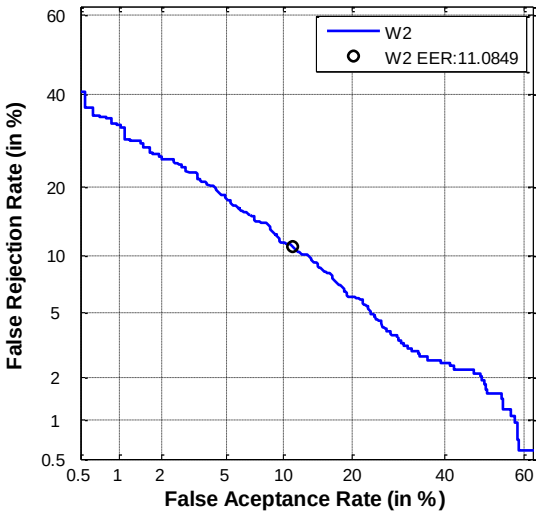


Figura 13: Ejemplo de una curva DET

En el eje de abscisas tenemos el FAR (False Acceptance Rate – Tasa de falsa aceptación) en porcentaje, mientras que en el eje de ordenadas el FRR (False Rejection Rate – Tasa de falso rechazo) también en porcentaje. El punto en el que cortan (señalado con un círculo en la leyenda de la parte superior de la *Fig. 14*), se trata del EER. En este caso, tiene un valor del 11.08% aproximadamente.

La nomenclatura que se ha usado en el desarrollo de los siguientes experimentos ha sido:

- **W2.** Tableta WACOM STU-530.
- **W5p.** Tableta Samsung Galaxy Note 10.1 en el caso de muestras recogidas con pen.
- **W5d.** Tableta Samsung Galaxy Note 10.1 en el caso de muestras recogidas con dedo.
- **W6.** Smartphone Samsung Galaxy SIII Neo.

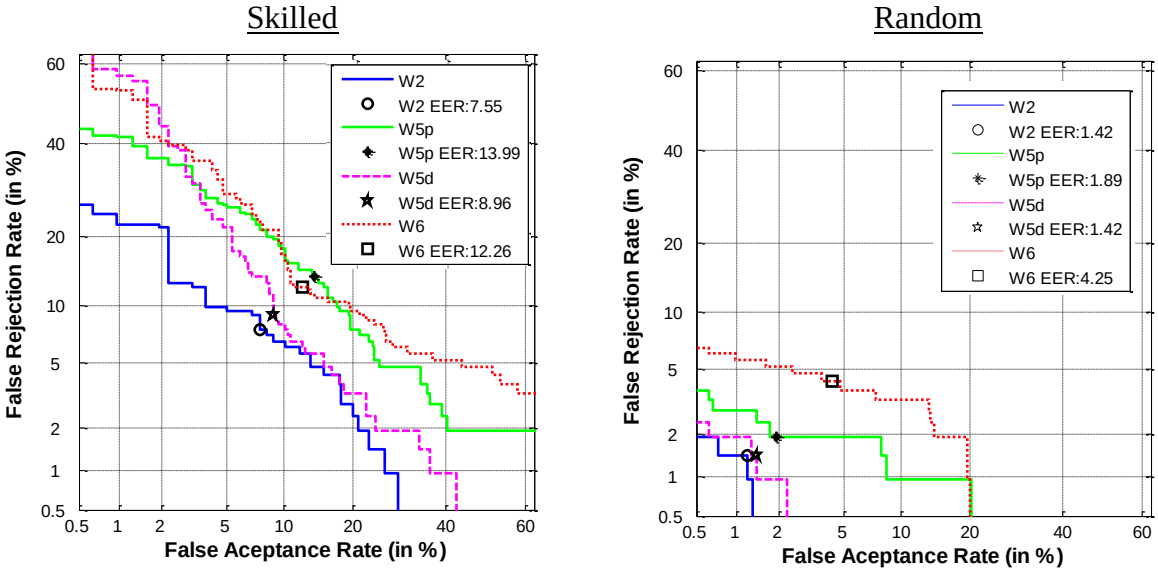
Por último, se estudiará la interoperabilidad entre todos los dispositivos. Este concepto de interoperabilidad ha recibido relativamente poca atención en la literatura. Algunos de los ejemplos encontrados en las diferentes modalidades biométricas se recogen en *[4][5][6][14][18]*.

4.3 Experimentos sin interoperabilidad

4.3.1 Pen contra dedo

En este experimento, se hace una comparación de los dispositivos que usan pen para la realización de la firma y los que usan dedo, con el objetivo de ver el rendimiento del sistema en los distintos casos.

Solo se mostrarán las gráficas de 4vs1 por ser las que tienen un valor de EER más bajo (demostrado en la *Sec. 4.3.2*).



(a) *(b)*

Figura 14: (a) curvas DET en el caso Skilled - 4vs1 - caso realista. (b) curvas DET en el caso Random - 4vs1. Ambas sustraídas de la base de datos e-Biofirma DS2

Como cabe esperar, se puede ver que en el caso random (Véase *Fig. 15 (b)*), se obtienen valores de EER mucho más bajos. Esto va a ocurrir siempre y para todos los casos según la definición de los conceptos de random y skilled vistos anteriormente. El sistema tiene más facilidad para rechazar a un usuario nuevo (no registrado en la base de datos) que intenta acceder con su firma genuina, que a un usuario que intenta acceder con una imitación de una firma ya registrada en la base de datos.

Por otro lado, se observa que en ambos escenarios el dispositivo que mejor funciona es el W2 (WACOM-STU530). Esto es lógico, ya que este dispositivo está diseñado exclusivamente para la captura de firmas.

Como se puede observar en el caso skilled (Véase *Fig. 15 (a)*), el W5d se encuentra en el segundo puesto de dispositivos con EER más bajos, seguido por el W6 y por último el W5p. Este dato es curioso ya que el siguiente dispositivo, después del W2, que se esperaba que fuese a tener un buen funcionamiento, es el W5p, debido a que los usuarios tienen más

costumbre a firmar con un lápiz que con el dedo. Sin embargo, este resultado demuestra que la tableta con sistema Android tiene buenas prestaciones en escritura con dedo.

En el caso random, también sorprende la presencia del dispositivo W5d en el segundo puesto. A continuación, se encuentra el W5p con un valor de EER de 1.89 y, bastante más alejado al resto, el W6. Este dispositivo, al igual que la tableta Samsung, no está diseñado para estos fines.

Media absoluta de mejora de los dispositivos que utilizan pen en el caso random frente al caso skilled: **9.115 %**
Media absoluta de mejora de los dispositivos con dedo en el caso random frente al caso skilled: **7.775%**

Esta media absoluta de mejora es menor en el caso de los dispositivos con dedo, ya que los valores que observamos en la gráfica también son menores.

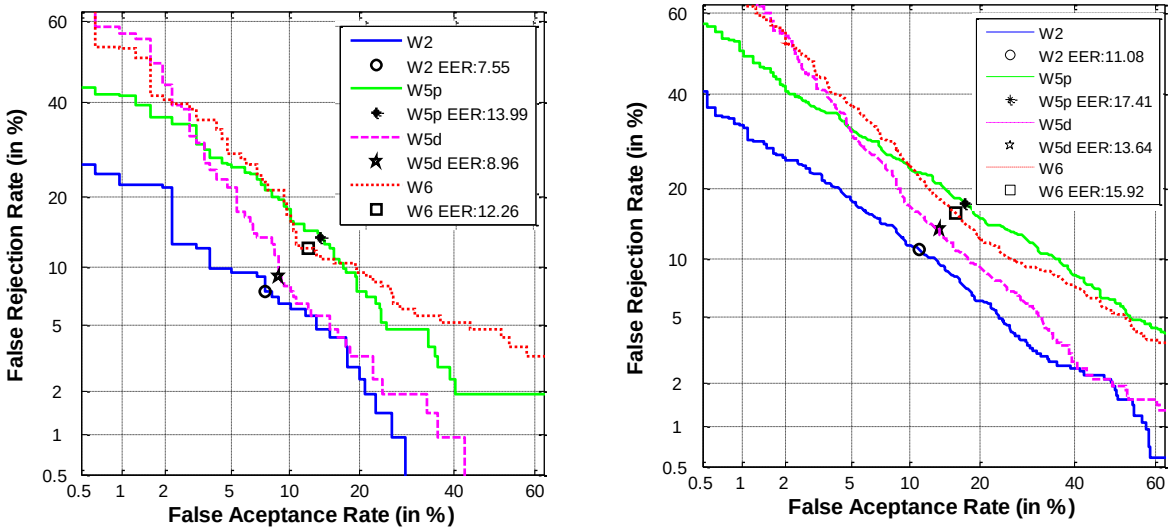
La conclusión que se puede extraer es que el W5d, a pesar de no ser un dispositivo diseñado para captura de firma manuscrita, obtiene buenos resultados en ambos escenarios. Por otro lado, el Smartphone es el dispositivo que peores resultados de rendimiento ofrece.

4.3.2 1vs1 contra 4vs1

En este experimento se compararán estos dos casos:

- **1vs1.** Entrenamos y testeamos el sistema con una muestra.
- **4vs1.** Entrenamos con 4 muestras y testeamos con una

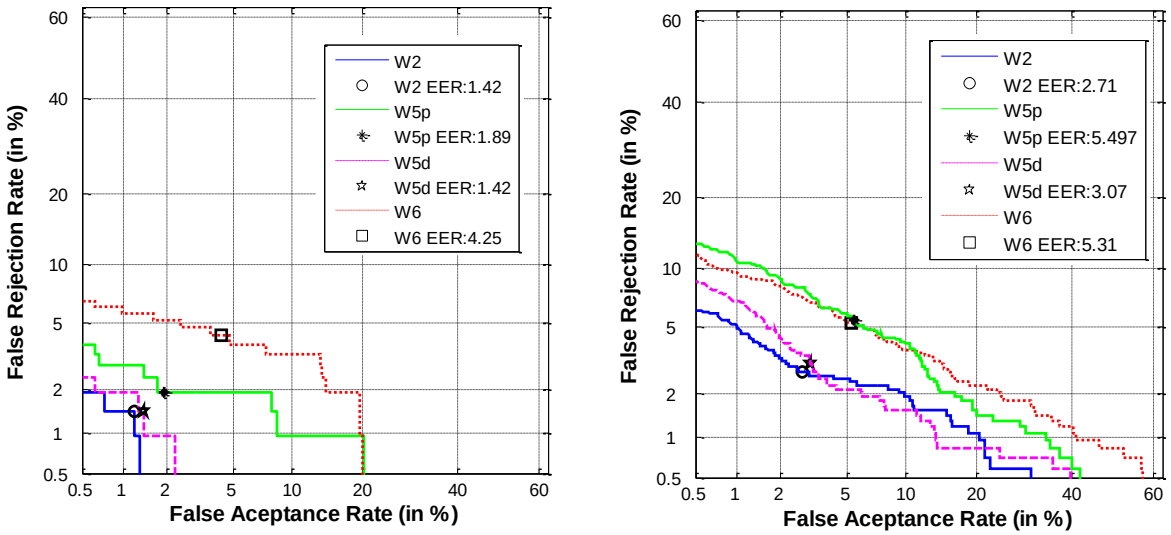
Skilled:



(a) *(b)*

Figura 15: (a) curvas DET en el caso Skilled - 1vs4 - caso realista. (b) curvas DET en el caso Skilled - 1vs1 - caso realista

Random:



(c) *(d)*

Figura 16: (c) curvas DET en el caso Random - 1vs4. (d) curvas DET en el caso Random - 1vs1

Analizando los resultados en este caso, vemos como en ambos escenarios, en el caso de entrenar al sistema con 4 muestras y testear con una (Véanse *Fig. 16 (a) y Fig. 17(c)*), se obtienen valores de EER menores.

La mejora absoluta en el caso skilled tiene un valor de **3.82%,** aproximadamente, mientras que en el caso random esta mejora es de **1.90%**.

Podemos concluir diciendo que el modelo 4vs1 obtiene mejores resultados que el caso 1vs1. Por lo que, para estudiar y analizar los experimentos se hará uso de este modelo.

4.3.3 Comparación de distintos tipos de imitaciones

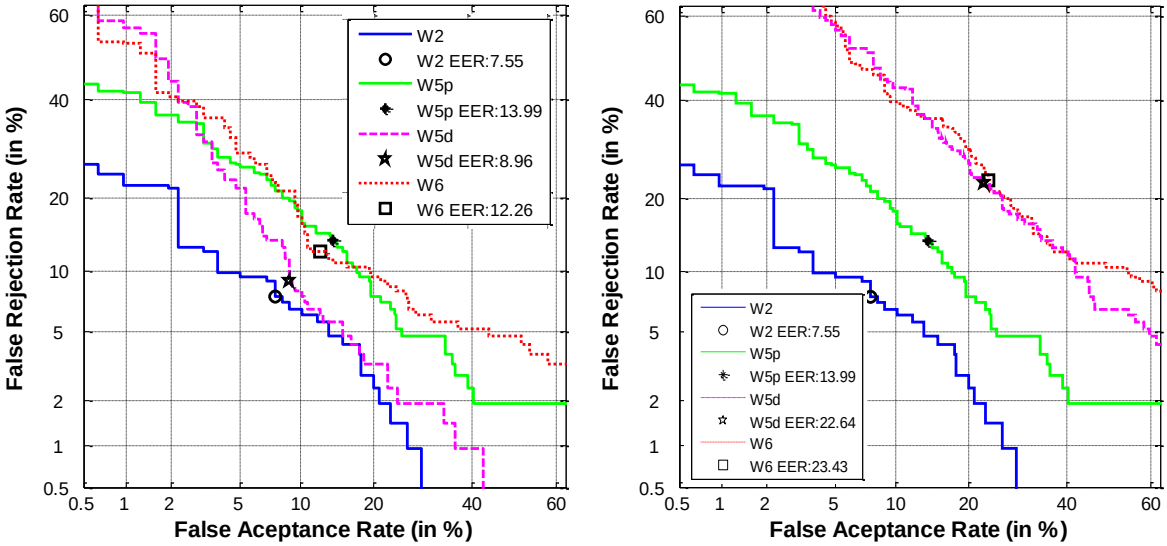
En este experimento se analizan dos tipos de situaciones:

- **Caso realista.** Este caso es el que se observa en la *Fig. 18 (a).* Las imitaciones capturadas por dispositivos que usan pen (W2 Y W5p) han seguido un proceso no realista. Se recuerda de la *Sec. 3.2,* que los usuarios tenían la posibilidad de ver la dinámica de la firma genuina a tiempo y velocidad real en la primera sesión, y la posibilidad de calcar esta firma genuina en la segunda sesión.

  Sin embargo, las imitaciones recogidas en el segundo bloque de ambas sesiones por los dispositivos que usan dedo (W5d y W6), se capturaron mediante el proceso realista descrito también en la *Sec. 3.2.* En este proceso, el usuario tenía la

posibilidad de ver la firma genuina impresa en un papel unos 30 segundos aproximadamente.
Solo se mostrarán las gráficas para el caso skilled ya que las firmas genuinas no cambian.

- **Caso no realista.** En este escenario (Véase *Fig. 18 (b)*), las imitaciones recogidas con pen van a ser las mismas que en el caso anterior. Y las imitaciones recogidas con dedo son aquellas que fueron capturadas mediante un proceso no realista, donde los usuarios podían visualizar la dinámica de la firma (Véase *Sec. 3.2*).



(a) *(b)*

Figura 17: (a) curvas DET en el caso Skilled – 4vs1 – realista. (b) curvas DET en el caso Skilled – 4vs1 – no realista

La diferencia entre el caso realista y el caso no realista, radica en los dispositivos que han capturado muestras con dedo (W5d y W6). En el caso de imitar la firma mediante una situación no realista, podemos observar como el valor de EER es más alto. Esto se explica debido a que las imitaciones en este caso son más parecidas a la firma genuina, debido a que los usuarios que realizaban las falsificaciones tenían más información acerca de ésta (como la dinámica y el tiempo de ejecución). El sistema en este caso, produce resultados mucho peores ya que tiende a confundirse más. Le es más complicado distinguir entre firmas genuinas reales contra falsificaciones reales.

La mejora absoluta en el caso realista es de **12.43%**, un valor bastante alto.

En las secciones anteriores de este capítulo, únicamente se han representado las curvas (que representan las imitaciones realizadas con los dispositivos W5d y W6) en el caso realista.

4.4 Experimentos con interoperabilidad

En esta sección, se intercambiará información entre varios dispositivos, utilizando para testear dispositivos diferentes que para entrenar.

4.4.1 Interoperabilidad entre dispositivos que utilizan pen

	Skilled 1vs4	
	Test	
Entrenamiento	W2	W5p
W2	7.55	26.3962
W5p	15.5660	13.99

	Random 1vs4	
	Test	
Entrenamiento	W2	W5p
W2	1.42	15.0943
W5p	25.4717	1.89

5: Valores de EER para dispositivos que usan pen. Interoperabilidad

Las conclusiones que se obtienen en el caso skilled son opuestas a las que se obtienen en el caso random.

Se tienen dos dispositivos, por un lado el W2 (diseñado para la captura de firmas) y por otro el W5p, el cual se ha demostrado en secciones anteriores que tiene un peor comportamiento a la hora de capturar firmas, ya que no está diseñado para este fin. Sin embargo, en este caso, se observa como al hacer una comparación con el caso anterior (sin interoperabilidad), en el caso skilled, los valores cruzados han aumentado al doble, mientras que en el caso random, estos valores aumentan hasta 8 veces más. Los valores que se obtienen al utilizar interoperabilidad entre estos dispositivos son mucho peores que sin utilizar interoperabilidad.

4.4.2 Interoperabilidad entre dispositivos que utilizan dedo

	Skilled 1vs4	
	Test	
Entrenamiento	W5d	W6
W5d	8.96	25
W6	23.5849	12.26

	Random 1vs4	
	Test	
Entrenamiento	W5d	W6
W5d	1.42	3.3019
W6	2.1045	4.25

6: Valores de EER para dispositivos que usan dedo. Interoperabilidad

En este caso se observa cómo es preferible entrenar al sistema con el W6 y testearlo con W5d en ambos escenarios. Esto demuestra que es preferible entrenar al sistema con un dispositivo de peores prestaciones, y utilizar durante el testeo un dispositivo más fiable, como es la tableta Samsung. Esta misma conclusión fue la que se obtuvo en el proyecto Fin de Carrera "Estudio de interoperabilidad en sistemas biométricos de firma manuscrita dinámica" desarrollado por Rubén Tolosana hace dos años.

Curiosamente, aunque ninguno de los dos dispositivos esté pensado para capturar firmas, se obtienen mejores resultados que en el caso anterior en el caso random, en el que se entrenaba al sistema con el W2 (dispositivo diseñado para la captura de firmas) y se testeaba con el W5p.

Por último, comparando los resultados obtenidos en el caso de no utilizar interoperabilidad, en el caso skilled, se observa como los valores cruzados son mucho peores, mientras que en el caso random los valores cruzados se mantienen respecto a los valores obtenidos sin utilizar interoperabilidad.

4.4.3 Interoperabilidad entre dispositivos que utilizan pen y dedo

El único dispositivo capaz de recoger muestras tanto con pen como con dedo es el W5 (Tableta Samsung), por lo que se considera el dispositivo más completo de la base de datos e-Biofirma DS2.

	Skilled 1vs4	
	Test	
Entrenamiento	W5p	W5d
W5p	13.99	35.6918
W5d	25.4717	8.96

	Random 1vs4	
	Test	
Entrenamiento	W5p	W5d
W5p	1.89	11.7925
W5d	11.3208	1.42

7: Valores de EER para dispositivos que usan pen y dedo. Interoperabilidad

Finalmente, este último experimento nos vuelve a demostrar que la base de datos del W5d utilizada para entrenar el sistema funciona bastante bien, obteniéndose valores de EER más bajos que si entrenamos al sistema con la base de datos del W5p. Sin embargo, se observa una gran diferencia en los valores obtenidos sin utilizar interoperabilidad frente a los valores cruzados, siendo éstos últimos mucho peores.

5| Conclusiones y trabajo futuro

5.1 Conclusiones

En este trabajo se ha conseguido cumplir el objetivo que se perseguía: adquisición de una base de datos (e-Biofirma DS2), de firma dinámica, con varios dispositivos fijos y móviles, y en varias sesiones.

El inminente desarrollo tecnológico hace imprescindible contar con bases de datos que proporcionen la información necesaria con respecto a la variabilidad existente entre capturas realizadas con diferentes y variados dispositivos que capturen un mismo rasgo biométrico; la existencia de este tipo de base de datos, ha permitido desarrollar sistemas de reconocimiento biométrico viables independientemente del dispositivo utilizado. Durante la realización del trabajo, se destaca el profundo estudio comparativo de los distintos dispositivos que han intervenido en esta base de datos y la motivación que ha llevado a estudiar la incorporación del smartphone como dispositivo de captura y su comportamiento. Estos dispositivos no afectan al correcto funcionamiento de sistemas de reconocimiento biométrico y ofrecen resultados positivos, sin embargo, se demuestra una vez más, que las tabletas WACOM siguen siendo punteras a la hora de capturar firmas digitales.

Otro tema predominante, ha sido el estudio de interoperabilidad, en el que se ha visto cómo es preferible entrenar al sistema con las firmas de un dispositivo menos fiable, y testear, posteriormente, con las firmas de un dispositivo con mejores prestaciones.

Por último, se ha intentado hacer frente al gran problema de seguridad: verificar si tú eres quien dices ser. La mejor alternativa a este problema es la verificación biométrica. Aunque todavía no se ha logrado resolver por completo, en este trabajo se ha aportado un riguroso estudio en el que se comparan diferentes casos con los diferentes dispositivos.

5.2 Trabajo futuro

Como trabajo futuro se proponen los siguientes objetivos:

- Ampliar el número de usuarios de la base de datos e-Biofirma DS2, para ofrecer resultados más realistas.

- Incluir nuevas sesiones para sujetos ya registrados en la base de datos e-Biofirma DS2 para observar de qué manera afecta a las firmas genuinas el paso del tiempo (observar el envejecimiento de la firma). Realizar una comparación y estudio de las muestras capturadas en la primera sesión de este proyecto con las nuevas muestras que se recojan.

- En relación al punto anterior, sería interesante analizar cómo influye el paso del tiempo a los sujetos de distintos rangos de edad. Es decir, observar si las firmas genuinas experimentan un mayor cambio en personas con mayor edad, o por el contrario, este cambio es más pronunciado en personas jóvenes.

- Por último, es importante desarrollar un sistema que lleve a cabo una compensación cuando se realiza interoperabilidad entre dispositivos, ya que los resultados en este proyecto son mejorables.

Referencias

[1] S.Gaytán, R.Vera-Rodríguez y J. Ortega-García. “Diseño y adquisición multi-dispositivo de base de datos de firma manuscrita dinámica”. Trabajo de Fin de Grado, Universidad Autónoma de Madrid (Escuela Politécnica Superior).

[2] Wacom Technology Corporation.” www.wacom.com”. WACOM STU-530. http://www.wacom.com/es-cl/enterprise/business-solutions/hardware/signature-pads/stu-530

[3] Anil K. Jain, Patrick Flynn, and Arun A.Ross. “Handlook of Biometrics”. Springer-Verlag New York, Inc.,Secaucus, NJ, USA, 2007.

[4] F. Alonso-Fernandez, J. Fierrez Aguilar, and J.Ortega-García. “Sensor interoperability and fusion in signature verification: A case study using tablet pc. In Proc. IWBRS, volume 3781 of LNCS.” 180-187. Springer, October 2005

[5] Arun Ross and Anil K.Jain. Biometric sensor interoperability: A case study in fingerprints. In Proc. ECCV Workshop BioAW, volume 3087 of “Lecture Notes In Computer Science”, 134-145. Springer, 2004.

[6] F. Alonso-Fernandez, R. N. J. Veldhuis, A. M. Bazen, J. Fierrez-Aguilar, and J-Ortega-García. “Sensor interoperability and fusion in fingerprint verification: A case study using minutiae-and ridge-based matchers. In Proc. IEEE Intl. Conf. on Control, Automation, Robotics and Vision, ICARCV, Special Session on Biometrics”, 422-427, December 2006

[7] Anil K. Jain, Arun Ross, and Salil Prabhakar. An Introduction to biometric recognition. IEEE “Trans. On Circuits and Systems for Video Technology”, 14:4-20, 2004

[8] Arun A Ross, Anil K Jain, and Karthik Nandakumar. “Handbook of Multibiometrics: Human Recognition Systems”. Springer, Dordrecht, 2006.

[9] Marcos Martinez-Diaz y Julián Fierrez. “Sinagure Databases and Evaluation”. Springer Verlag, Julio 2009

[10] J- Galbally, J. Fierrez, y J.Ortega-García. Bayesian hill-climbing attack and its application to signature verification. In Proc. IAPR “International Conference on Biometrics, ICB”, volume 4642 of LNCS, 386-395. Springer, Agosto 2007

[11] J. Fierrez-Aguilar, L. Nanni, J. Lopez-Peñalba, J.Ortega-Garcia, and D.Maltoni. “An on-line signature verification system based on fusion of local and global information”. In Proc. 5th IAPR Intl. Conf On Audio- and Video-based Biometric Person Authentication, AVBPA, volume 3546 of LNCS, 523-532. Springer , Julio 2005.

[12] Hiroaki Sakoe and Seibi Chiba. Dynamic programming algorithm optimization for spoken word recognition. IEEE “Transactions on Acoustics, Speech, and Signal Processing”.(1):43-49, 1978

[13] Marcos Martinez-Diaz. “Dynamic signature verification for portable devices. Master’s thesis”, Universidad Autónoma de Madrid, Noviembre 2008

[14] R- Tolosana-Moranchel, R. Vera-Rodriguez, J.Ortega-García. “Estudio de interoperabilidad en Sistemas Biométricos de firma manuscrita dinámica” 24(Tabla 3.1). ATVS Grupo de Reconocimiento biométrico. Universidad Autónoma de Madrid (Escuela Politécnica Superior), Proyecto Fin de Carrera Octubre 2014.

[15] Julián Fierrez, Javier Ortega-garcía, Daniel Ramos, y Joaquín Gonzalez-Rodriguez. “Hmm-based on-line signature verification: feature extraction and signature modelling. Patern Recognition Letters”, 28(16):2325-2334, Diciembre 2007

[16] Daigo Muramatsu and Takashi Matsumoto.” An hmm on-line signature verifier incorporating signature trajectories.” In Proc. ICDAR, 438-442. IEEE Computer Society, 2003.
[17] K.N. Platanioitis, C.S. Regazzoni (eds.), “Special Issue in Visual-centric Surveillance Networks and Services”, IEEE Signal Processing Magazine, 22(2), Marzo 2005.
[18] R. Tolosana, R. Vera-Rodriguez, J. Ortega-Garcia y J. Fierrez, “Preprocessing and Feature Selection for Improved Sensor Interoperability in Online Biometric Signature Verification”, IEEE Access, Vol. 3, 478 – 489, Mayo 2015.

Anexos

A Dispositivos de captura

En este anexo, se explicará con detalle cada una de las características principales de cada dispositivo que ha intervenido en la adquisición de la base de datos.

A.0.1. WACOM STU-530: *[2]*

Esta tableta ofrece una experiencia de firma muy cómoda con un diseño mejorado. Podemos destacar las siguientes características:

- Frecuencia de muestreo: 200Hz (5ms/muestra).
- Pantalla LCD de color de 5'' con resolución de 800 x 480.
- Proporciona un lápiz inalámbrico (pen) y sin pilas patentado, con 1024 niveles de sensibilidad a la presión para una mejor captura. Este lápiz cumple con normas legales.
- Aprobación de pruebas de uso rigurosas para capturar más de 500.000 firmas sin desgaste de la superficie.
- Cifrado AES con el objetivo de realizar transacciones seguras.
- Identificación única de hardware con el fin de identificarse el dispositivo exacto utilizado para la firma.
- Captura de firmas electrónicas a mano jurídicamente vinculantes.

(a)

A.0.1. SAMSUNG GALAXY NOTE 10.1 (ANDROID):

Se trata de una Tablet con una pantalla Full HD de 10.1''. Especificaciones técnicas:

- Cuenta con una pantalla de increíble resolución WQXGA.
- Número de colores: 16 M.
- Resolución: 1600 x 2560.
- En este caso, por primera vez en la gama de dispositivos Samsung Galaxy Note, es prescindible el uso del lápiz digital táctil.

(b)

A.0.1. SAMSUNG GALAXY S III NEO:

Este Smartphone lo describen en tres palabras: Intuitivo, Comparte y Rendimiento. Entre las especificaciones técnicas tenemos:

- Tecnología HD sAMOLED.
- Tamaño 4.8’’.
- Resolución: 720 x 1280 (HD).
- Número de colores: 16 M.
- Sensores: Acelerómetro, geomagnético, giroscopio, luz RGB, barómetro.
- Dimensiones Físicas (AlxAnxProf): 136.6x70.7x8.6 mm.
- Peso: 132 g.
- Prescindible uso de S Pen.

(c)

Figura 18: (a) Tableta WACOM – STU530. (b) Tableta Samsung Galaxy Note 10.1. (c) Smartphone Samsung Galaxy SIII Neo

B Dificultades durante la adquisición

En este anexo se van a detallar los problemas que hubo en el proceso de adquisición de datos. Es altamente recomendable que estos problemas se solucionen en futuros proyectos.

- En un primer momento, se pensó que la base de datos incluyese 80 personas del CAU (Centro de Atención a Usuarios) situado en la Universidad Autónoma de Madrid, y 20 personas de primer curso de Programación I. En la primera sesión, se llegó a 79 usuarios en total, sin embargo, al realizar la segunda sesión, solo 53 de estos 79 completaron la segunda sesión.

- La separación entre la primera sesión y la segunda, se esperaba que fuese de 3 semanas como mínimo. Se tuvo que reducir esta variable a dos semanas ya que se necesitaba la base de datos completa de forma urgente.

- Las falsificaciones, que en un primer momento estaban pensadas para que las realizasen los usuarios ya registrados, finalmente se realizaron por compañeros del ATVS.

- Cuando se procedía a realizar, de forma manual, la secuencia alfanumérica, la letra del DNI cambiaba con respecto a la realizada en el proceso automático.

- Cuando se les solicitaba a los usuarios que escribiesen su nombre y primer apellido, escribían, de forma involuntaria, los dos apellidos. Esto empeoró nuestro sistema y el proceso de adquisición se hizo más largo.

- Por último, tras obtener toda la base de datos y proceder a la revisión de ésta, se detectó un error de programación. En los dispositivos W5 (Tablet) y W6 (Smartphone), la imitación realizada por el último usuario era incorrecta (p.ej. si se está en la carpeta “forgeries” del usuario 105, sería la falsificación que realizó el usuario 108), siendo ésta la del usuario anterior. Sin embargo, esto no ocurre para todos los usuarios, pero si para casi todos. Los usuarios que no presentaron ninguna alteración de este tipo, tanto en la tableta Samsung como en el Smartphone, fueron: 107, 109, 117, 119, 127, 129, 137, 139, 147, 149 y 153.